Data Transmission & Storage Standard
St. Bonaventure University

Scope: These guidelines apply to all information systems storing or transmitting University data off the University network.

Requirements:

1. Transmission:
   - Critical and highly sensitive data must be transmitted using email encryption or SFTP (secure file transfer protocol).
   - It is recommended that email encryption, SFTP (secure file transfer protocol), or SSL encryption be used when transmitting moderately sensitive data.
   - Employees using the SBU wireless must access the secure wireless network (SBUSEC) to transmit any highly or critically sensitive data.
2. Storage:
   - Critically sensitive data may only be stored and shared by designated servers and/or applications (such as Colleague or Raiser's Edge).
   - Highly sensitive data may only be stored on a file and/or web server with appropriate access controls (such as SBU share drive).
   - Users may store highly or moderately sensitive data on their SBU owned desktop or encrypted laptop.
   - Any files that meet the highly sensitive or critically sensitive level in data classification may only be stored on a secured SBU server/computer or a trusted 3rd party solution certified by the Chief Information Officer.

Implementation Guidance:

1. File transfers
   - Encrypted file transfers can be done by using an encrypted transmission protocol or service such as SFTP (secure file transfer protocol). If an unencrypted mechanism is used to transfer a file containing sensitive data, the file must be encrypted before being transferred. Information Technology provides assistance with SFTP transfers for all faculty, and staff.

2. Web Applications
   - Sensitive data communicated between a web application and the client machine should be encrypted using TLS/SSL or other secure protocols. This can be determined by looking at the URL of the site you are sending data from. If the URL contains "https" then you are ok, however if it is only "http" please be cautious.

3. Email
   - Regular email is not considered a secure method for sharing critically sensitive data.

- No SBU email (internal or external) will include data that meets critically sensitive level in data classification

4. Virtual Private Network
    - The university provides a virtual private network that can provide encrypted access to services that don't offer encryption services natively. VPN is provided upon request to employees with university computers at openvpn.sbu.edu.